Uma Abordagem de Senha Gráfica para Controlo de Acessos na Web

An Approach Password Graphic for Access Control Web

Nelso P. C. Ventura
Instituto Politécnico de Beja
Beja, Portugal
nelso.ventura@gmail.com

Luís Carlos Bruno
Instituto Politécnico de Beja
LabSI2
Beja, Portugal
lbruno@ipbeja.pt

Resumo - **Este artigo descreve a investigação de uma abordagem inovadora de um modelo de senha gráfica que suporta a autenticação segura em sistemas Web e que pretende solucionar o problema do espião de ombro. Para tal, desenvolveu-se um novo modelo de senha gráfica, baseada na imagem da página Web, que o utilizador tem aberta no momento em que efetua o seu registo de utilizador, e sobre a qual são desenhados traços, com dimensões, direções, e sequências, à sua escolha. Num estudo exploratório com participantes, que simularam ser espiões de ombro, verificou-se que mais dificilmente se perceciona quando um utilizador se autentica, usando uma senha gráfica, do que utilizado uma senha alfanumérica. O modelo de senha gráfica proposto foi desenhado iterativamente e centrado no utilizador. Para validar a sua segurança e usabilidade, foram feitos vários testes com participantes. Nesses estudos, pretendeu-se perceber o grau de eficácia e de memorização que este modelo de senha gráfica inovador proporciona aos utilizadores em ambiente Web. Os resultados obtidos mostraram que se obteve uma solução segura e usável, com potencial para ser usado em alternativa à senha alfanumérica, por forma a evitar o risco do espião de ombro.**

Palavras Chave - Senhas Gráficas; Senhas Alfanuméricas; Memorização; Vulnerabilidades; Segurança;Autenticação na Web

Abstract — **This article describes the research of an innovative approach to innovative graphical password model that supports secure authentication in Web systems and wants to solve the shoulder spy problem. To this end, we developed a graphical password model based on two elements: a Web page image that the user has opened in the moment of its enrolment, and strokes drawn with dimensions, directions, and sequences of user choice's. In an exploratory study with participants to validate shoulder spies perceptions, it was found that are more difficult when a user is logging in using a graphical password, than when using an alphanumeric password. The model was designed iteratively and user-centered. To validate its safety and usability, they were made several tests with participants. In these studies, we tried to understand the degree of effectiveness and memorization provided by this password graphical model to users in Web authentication. The results showed that we got a usable and secure solution with potential to be used as an alternative to alphanumeric password, against the shoulder spy in Web authentication.**

Keywords - Graphical passwords; Alphanumeric passwords; memorization; vulnerabilities; Security; Web Authentication

1 INTRODUÇÃO

Os métodos de autenticação para o acesso a sistemas informáticos e de comunicações são normalmente baseados no identificador do utilizador e numa senha alfanumérica. Esta é baseada numa sequência de letras, números, e outros caracteres, daí terem a designação de alfanumérica.

Este tipo de senha tem a desvantagem de motivar o utilizador a gerar senhas fáceis de descobrir [1]. Por outro lado, se forem geradas automaticamente, tornam-se difíceis de relembrar. Desta forma, ele tende a escrever a senha em locais acessíveis a outras pessoas, o que pode causar problemas de segurança. Por outro lado, a introdução deste tipo de senha pode estimular um espião de ombro a espreitar as ações que o utilizador efetua com o teclado e/ou rato. Um outro modelo alternativo é o da senha gráfica, que explora a memória visual do utilizador. Já existem alguns exemplos comerciais, como são o caso do padrão Android Unlock [2], ou do Windows 10 [3].

Após uma análise do estado da arte, da área das senhas gráficas, identificaram-se alguns problemas em aberto, como por exemplo, o número de imagens a utilizar, a carga gerada na rede, a atividade nos servidores e as questões de segurança. Identificou-se um problema de segurança comum aos estudos analisados e que é independente da qualidade da senha: a obtenção indevida da senha por um espião de ombro que observa o utilizador a introduzir os seus caracteres através de um teclado físico ou de ecrã.

Para que isso não aconteça, será importante que o espião de ombro não tenha indícios de que o utilizador está a executar uma operação de autenticação. Neste estudo, colocámos a hipótese de que a senha gráfica possa mascarar melhor a tarefa de autenticação do espião de ombro, do que a

senha alfanumérica. Esta hipótese foi validada por um estudo exploratório com participantes que simularam ser espiões de ombro em páginas Web. Assim, arguimos que as senhas gráficas podem ser uma proposta alternativa efetiva às senhas alfanuméricas, sem prejuízo de critérios de usabilidade e de segurança [4] exigidas para sistemas de controlo de acessos.

Na sequência deste resultado, definiu-se um modelo de senha gráfica, desenvolvida iterativamente, centrada no utilizador, e baseada num conjunto de regras. A senha gráfica proposta é suportada numa imagem de fundo, gerada automaticamente a partir de uma página do sítio Web, e sobre a qual é feita a autenticação. A imagem funciona como um contentor de objetos, constituído por imagens, caracteres, palavras, frases e letras, que suporta o desenho dos elementos que constituem a senha gráfica.

Após terem sido desenvolvidos vários testes com participantes, definiu-se um modelo de senha gráfica constituído pelo desenho de seis traços, com tamanho, direção e sequência à escolha do utilizador. Participaram nos testes um leque abrangente e heterogéneo de utilizadores, que garantiram representatividade do público-alvo deste tipo de tarefas. Os resultados obtidos mostraram que se obteve um modelo final de senha gráfica com potencial para ser usado em alternativa à senha alfanumérica, assegurando eficácia, facilidade de utilização e de memorização ao utilizador, e com a vantagem de oferecer uma maior segurança contra o espião de ombro.

Na secção "Estado da Arte", são apresentadas e discutidos os principais trabalhos na área das senhas gráficas, e de alguns de outros tópicos que lhe estão relacionados. Na secção "Análise do Problema", apresenta-se um estudo exploratório, que mostra o potencial da senha gráfica para combater a ameaça do espião de ombro. Na secção "Desenho de modelo de senha gráfica para a Web", são relatadas as várias versões do modelo da senha gráfica que foram desenvolvidas, suportados em testes com participantes. Na secção "Conclusões e Trabalho Futuro", sintetizam-se os principais resultados obtidos, e os próximos passos nesta investigação.

2 Estado da Arte

Durante a década de 1960, as primeiras senhas alfanuméricas foram introduzidas, como uma solução para resolver as questões de segurança em acesso a sistemas multiutilizador.

As senhas alfanuméricas são simplesmente uma sequência de letras, caracteres e algarismos, que, quando combinadas, podem criar uma senha segura. Após vários estudos [5] [6], chegou-se à conclusão de que deve haver um certo conjunto de características na construção de uma senha alfanumérica segura. Esta deve conter pelo menos oito caracteres; não ter dados relacionados com o utilizador (por exemplo, o nome, sobrenome ou a data de nascimento), não ser uma palavra que pode ser facilmente encontrada num dicionário, e possuir uma combinação de letras maiúsculas e minúsculas, caracteres especiais e números. Um estudo anterior [7] demonstra que mais de 80 % dos utilizadores já acederam sem autorização, a informação privilegiada, assim como já foram vítimas do espião do ombro no local de trabalho, usando senhas alfanuméricas. Neste sentido, algumas técnicas baseadas em reconhecimento foram concebidas para resistir a este tipo de ataque [8] [9]. Com o aumento exponencial dos sistemas em rede, tem sido pertinente estudar outros tipos de senhas, como é o caso da senha gráfica.

Vários modelos de senha gráfica têm sido propostos. Algumas técnicas de criação de senhas gráficas, têm sido desenvolvidas com o objetivo de facilitar a utilização de senhas gráficas em vez das alfanuméricas [10] [11] [12] [13] [14]. As senhas gráficas baseadas em reconhecimento tendem a ser suficientemente pequenas e fáceis para que seja possível o utilizador memorizar e lembrar. E é mais difícil realizar um ataque de força bruta, contra senhas gráficas do que contra senhas baseadas em texto. Para algumas senhas gráficas baseadas em recordação humana [10] [15], é possível usar um ataque de dicionário, mas quando automatizado é muito mais complexo e demorado que um ataque de dicionário baseado em texto.

Alguns dos modelos desenvolvidos de senhas gráficas foram baseados em técnicas de visualização, recorrendo a funções Hash [16], e outros suportaram autenticação em técnicas de pergunta/resposta com imagens aleatórias [17]. Estes modelos revelaram pontos fracos, no armazenamento seguro do caminho das imagens, permitindo o ataque por dicionário e na lentidão do sistema por via do carregamento de imagens. O reconhecimento de imagens baseado num vasto conjunto hipóteses [18], mostraram também algumas fragilidades na memorização dessa informação, que desmotiva o utilizador a usar essa técnica. A técnica de autenticação utilizada no sistema Passface [19], mostrou anomalias de utilização, porque a maioria dos utilizadores tendem a escolher os rostos de pessoas com atributos parecidos, tornando-o previsível nas escolhas. Este problema pode ser atenuado através da atribuição aleatória de rostos, mas isso, mais uma vez, tornaria difícil a sua utilização porque se perde o padrão de memorização. As técnicas de autenticação são vulneráveis ao espião de ombro. Tome-se como exemplos, os casos da inserção do PIN numa caixa multibanco, ou num terminal POS. A técnica do espião do ombro também pode ser feita à distância, utilizando dispositivos que permitem melhorar a visão, como por exemplos as câmaras de vigilância. Existem estudos sobre o tema [20] que pretendem colmatar este problema com a senha gráfica. A utilização de imagens ou objetos pré-selecionados pelo utilizador é uma proposta interessante para reforçar a memorização, mas com a sua continuada utilização, o espião do ombro tende a perceber que está em presença de um processo de autenticação. A vulnerabilidade do espião do ombro continuou a ser estudada, e novos sistemas são propostos. Histórias ou cenas com imagens para criar as senhas são estudadas [9], mas os utilizadores continuam a ter vários problemas de memorização, reconhecimento e identificação, o que torna os sistemas lentos e vulneráveis. Para colmatar estas limitações foram criados dicionários gráficos [10] [21], foram definidos parâmetros do

comprimento de senhas gráficas, e imagens em grelhas Cognometric Scheme [22] [23]. Uma das abordagens mais interessantes definiu que o utilizador devias escolher como referencia um mínimo de objetos propostos ou seja pequenos pontos da imagem, a considerar na senha gráfica [24]. Vários estudos com utilizadores mostraram que existem características comuns no desenho da senha gráfica, o que a torna vulnerável. A técnica desenvolvida no Passdoodle [11] consiste na criação da senha gráfica com o recurso a um desenho de objetos com uma caneta sobre um ecrã sensível ao toque, onde se pode concluir que os utilizadores foram capazes de recordar as imagens assim como recordam as senhas alfanuméricas. Os estudos com utilizadores também mostraram que as pessoas tendencialmente têm dificuldades em se lembrar da ordem pela qual desenharam a sua senha. Clicar em vários locais de uma imagem com alguma tolerância [25], pode ser uma hipótese que permite ajudar o utilizador a recuperar a senha, tornando este método mais conveniente do que a recordação. O estudo desenvolvido no Passlogix [26], no qual o utilizador clica em vários pontos de uma imagem, numa sequência correta, oferece-lhe uma margem de erro para cada item, com o objetivo de o ajudar na sua autenticação. Uma técnica similar foi desenvolvida pela Microsoft [27], onde a senha [28] do utilizador é composta por três pontos sobre uma imagem, numa ordem específica. Esta técnica já está a ser utilizada no Windows 10 [27] [23]. Embora tenha vulnerabilidades de segurança [29], é considerado um sistema divertido de ser usado. Por fim, e não menos interessante, estudou-se o sistema PassPoint [35] [30], baseado no método de diferenciação proposto em [15], e que é uma evolução das senhas gráficas [25], permitindo a utilização de imagens escolhidas livremente pelo utilizador, podendo clicar em qualquer ponto da imagem, sem estar restringido a áreas pré-definidas. Este sistema permite uma margem de tolerância de erro em pixel relativa a cada ponto escolhido, bem como requer a validação na sequência correta [31]. O Passpoint melhora vulnerabilidades de ataque por força bruta e do espião do ombro, suportados no tempo de autenticação cronometrado [22]. No entanto, foram identificadas algumas dificuldades da sua memorização e utilização.

Salvaguardando poucas exceções [8] [9] [32], [33], existem dificuldades em capturar a senha gráfica por aplicações spyware, que tentem detetar as ações do teclado e do rato. Para que a senha seja capturada é necessário que o sistema tenha informação de contexto, como sejam, a posição e o tamanho da janela, e tempo permitido para a autenticação. O ataque por engenharia social, ação que explora as falhas de segurança por manipulação do utilizador [34], pode ser um risco inferior quando suportado numa senha gráfica, porque essa informação verbal é menos rigorosa quando transmitida a outrem. No geral, acredita-se que é muito mais difícil descobrir a senha gráfica usando os métodos tradicionais, do que a senha alfanumérica.

Esta análise do estado da arte inspirou este trabalho para o desenvolvimento de um modelo de senha gráfica que evite o risco do ataque por espião de ombro, que seja fácil de utilizar, assegurando níveis corretos de eficácia e de memorização ao utilizador, e reduzindo ao máximo a troca de informação entre o cliente e o servidor, no contexto Web.

3 Análise do Problema

A autenticação de utilizadores em sítios e aplicações na Web é muito comum para restringir o seu acesso somente aos utilizadores que têm permissões para usar os seus recursos.

Uma página de autenticação comum na Web, é facilmente reconhecida por um observador externo, através da observação de duas caixas de texto, associadas a um botão de validação. Uma das caixas permite introduzir o nome do utilizador, e a outra permite inserir uma senha alfanumérica, com caracteres normalmente mascarados. Isto leva a que um espião de ombro perceba facilmente que operação o utilizador está a realizar, motivando-o a tentar decifrar os dados de autenticação, através da observação das ações com o teclado e da informação presente no ecrã. Sítios de *homebanking*, de *webmail* e de redes sociais, que normalmente mantêm sempre a mesma estrutura e aparência nos controlos da autenticação alfanumérica, chamam mais a atenção aos espiões do ombro. Como alternativa às senhas alfanuméricas, existem as senhas gráficas, que também têm algumas vulnerabilidades de segurança e alguns problemas de utilização. Normalmente, o utilizador tende a usar registos muito comuns sobre as imagens da senha gráfica, como por exemplo, os olhos, a boca, e o nariz, nas faces humanas. Isto gera vulnerabilidades que podem ser exploradas por decifradores de senhas. Alguns sistemas usam uma grande quantidade de imagens aleatórias, que tornam os sistemas lentos na transmissão desses dados para o lado do cliente, o que perturba a utilização e a memorização do utilizador. Estes problemas de usabilidade, desmotivam o utilizador a utilizar esse tipo de método de senhas gráficas.

A. Teste exploratório do espião de ombro

No início desta investigação desenvolveu-se um estudo inicial que pretendeu aferir qual é o nível de perceção que uma pessoa comum, tem sobre a realização da tarefa de autenticação em dois cenários distintos. Um deles usa o sistema clássico, suportado numa senha alfanumérica. O outro é suportado numa senha gráfica. Pretendeu-se simular a tarefa do espião de ombro, interrogando-se cada participante sobre qual era a ação que ele estava a visualizar para cada um dos dois cenários. Participaram no estudo quarenta e nove participantes, em dois momentos diferentes. Eles observaram a utilização de duas diferentes páginas Web (ver Figura 1 e a Figura 2) numa tela de projeção. Cada uma dessas duas páginas foi controlada pelo moderador do estudo, que executou diferentes operações de manipulação do cursor do rato e do teclado, para ilustrar os dois cenários de autenticação. No final da observação de cada uma das páginas Web, cada participante foi inquirido para identificar que tipo de ações/tarefas é que o moderador tinha efetuado.

Na Figura 1 é representada a página que simula o cenário de uma autenticação baseada numa senha gráfica. Na Figura 2 é ilustrado o cenário da autenticação baseada numa senha

alfanumérica, tal como a presença das duas caixas de autenticação indicia ao utilizador.

Figura 1– Página Web que simula a autenticação com senha gráfica

Na sequência da inquirição feita aos participantes, verificou-se para o caso da simulação do cenário da senha gráfica, que nenhum dos quarenta e nove indivíduos percionou que o utilizador estava a fazer uma operação de autenticação. Por outro lado, a maioria deles (76%) responderam que o utilizador estava simplesmente a navegar na internet. Relativamente à simulação do uso da senha alfanumérica, vinte e cinco (51%) dos sujeitos responderam que o utilizador estava a realizar uma tarefa de autenticação.

Figura 2 – Página Web que simula a autenticação da senha alfanumérica

Os resultados mostrados na Figura 3 mostram que não é claro para um espião do ombro, que o utilizador esteja a efetuar uma operação de autenticação, se ele não recorrer ao padrão comum da autenticação baseado na senha alfanumérica. Por outro lado, usando esta técnica, é evidente, para a maioria dos espiões de ombro, que o utilizador está a efetuar uma operação de autenticação.

Figura 3 – Resultados do inquérito da simulação do espião de ombro nos cenários da senha gráfica e alfanumérica

Estas conclusões levaram à convicção de que o uso da senha gráfica pode despistar os espiões de ombro, quando o utilizador está a realizar a tarefa de autenticação na Web. Esta questão motivou este trabalho a tentar encontrar um modelo de senha gráfica, alternativa à senha alfanumérica, no contexto da Web, e que seja segura e usável para o utilizador.

4 Desenho de modelo de senha gráfica para a Web

Para desenvolver um modelo de senha gráfica adaptada aos requisitos definidos previamente, foram inicialmente definidos vários princípios orientadores do seu desenho. A primeira proposta de modelo de senha gráfica, foi baseada nas decisões de desenho seguintes:

- A senha gráfica tem como base uma imagem, obtida a partir de uma página desse sítio Web, no momento em que for feito o seu registo;
- Sobre essa imagem podem ser desenhados oito objetos geométricos com as características seguintes: segmentos de reta, polígonos e círculos, numa sequência definida livremente pelo utilizador.

A escolha de oito objetos para construir a senha, baseou-se na lógica da utilização do mesmo número de oito caracteres, que é usado nas senhas alfanuméricas.

Para validar os princípios do desenho enunciados anteriormente, foi feito um teste com utilizadores que pretendia verificar qual o grau de acerto e de memorização das senhas gráficas por eles registadas anteriormente.

Usando a aplicação de desenho MSPaint[tm], catorze participantes do teste criaram oito objetos (polígonos, segmentos de reta, ou círculos) sobre a imagem de uma página Web, na sequência e nas posições pretendidas, conforme é mostrado na Figura 4. Foi-lhes pedido que memorizassem essas ações, para as tentarem reproduzir, passadas seis horas, com a mesma sequência e o mesmo posicionamento dos objetos sobre a imagem.

Figura 4 – Exemplo de registo de objetos gráficos sobre imagem de página Web

Com base na observação e no registo das suas ações, verificou-se que a esmagadora maioria dos participantes teve grandes dificuldades em reproduzir os mesmos objetos sobre imagem base, e com a mesma sequência, conforme os resultados expressos na Figura 5.

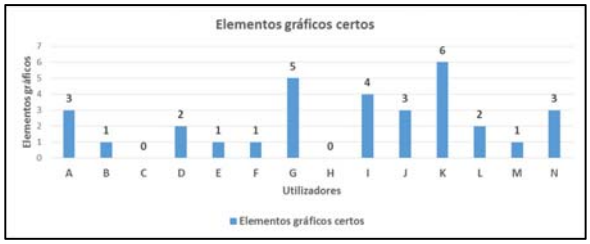

Figura 5 – Resultados dos testes sobre a primeira versão do modelo de senha gráfica

Verificou-se que nenhum dos sujeitos conseguiu reproduzir na totalidade os oito objetos registados (o máximo de acertos foi de seis objetos), e na maioria deles, oito em catorze (57%), teve dois ou menos acertos.

Este teste demonstrou que a primeira versão de modelo proposto apresentou vários problemas de usabilidade, assentes em dificuldades na memorização da geometria dos objetos, no seu posicionamento e na sequência em que são registados. Isto motivou o desenvolvimento de um modelo redesenhado da senha gráfica, que melhor se pudesse adequar aos seus utilizadores.

A. Redesenho e avaliação da senha gráfica

Na sequência da análise dos resultados obtidos na primeira versão de senha gráfica, decidiu-se redesenhar o seu modelo, alterando alguns dos seus princípios do desenho.

Para reduzir a complexidade da geometria dos objetos usados (polígonos, segmentos de reta, ou círculos), decidiu-se usar somente segmentos de reta, em virtude de serem descritos somente por duas coordenadas, por cada ponto extremo, o que requer menos capacidade de memorização. Por esta última razão, o número de objetos desenhados foi também reduzido de oito elementos gráficos para seis.

Manteve-se o conceito da imagem de fundo que permite que, diferentes utilizadores, registem diferentes imagens na sua conta de utilizador do sistema.

Figura 6 – Desenho dos segmentos de recta sobre a imagem

Na sequência do redesenho efetuado, foram feitos testes com utilizadores para avaliar a usabilidade desta nova versão de senha gráfica. Pretendeu-se com estes testes avaliar a memorização da informação respeitante aos registos dos segmentos de retas, para períodos de média (6h), e de mais longa duração (72h). A informação que os participantes memorizam corresponde às posições dos seus dois pontos extremos, definidos no sistema de coordenadas bidimensionais da imagem em causa.

Três testes foram realizados em tempos diferentes. O primeiro teste (teste 1) teve vinte e sete participantes. O segundo teste (teste 2) teve vinte e oito participantes (vinte e sete foram comuns com o teste anterior), e o terceiro teste teve os mesmos vinte e oito participantes. Inicialmente, foi-lhes proposto registarem à sua escolha, seis segmentos de reta, com tamanhos e com direções, sobre uma imagem predefinida, retirada de um jornal eletrónico, conforme é exibido na Figura 6. Esta tarefa foi suportada na utilização do programa MSPaint[tm].

No **teste1**, os participantes não foram informados de que deveriam memorizar as posições dos traços registados previamente. No entanto, passados seis horas, foi-lhes solicitado que reproduzissem os mesmos seis segmentos de reta sobre a mesma imagem.

Na Figura 7, é possível verificar que a maioria dos participantes (59%), correspondentes a dezasseis em vinte e sete, não conseguiu reproduzir corretamente nenhum dos segmentos de reta, e que somente quatro utilizadores reproduziram corretamente os seis segmentos de reta.

Figura 7 - Respostas certas sem conhecimento do teste

A esmagadora maioria dos utilizadores teve muita dificuldade em lembrar-se do padrão dos elementos gráficos registados 6h antes. Isto mostrou que se não houver uma motivação forte para reter este tipo de informação visual, então os utilizadores têm dificuldades em a reproduzir posteriormente.

No **teste 2**, foi solicitado aos participantes que registassem os seis segmentos de reta sobre a mesma imagem do teste anterior, mas, desta vez, foram informados de que deviam memorizar as posições dos segmentos de reta. Passadas 6h, os participantes foram convocados para tentar reproduzir os segmentos de reta desenhados previamente.

Na Figura 8, é possível verificar que 64,3% (dezoito em vinte e oito) dos participantes acertou os seis segmentos de reta, e que 78,2% (vinte e dois em vinte e oito) acertaram em quatro ou mais segmentos de reta.

Figura 8 – Respostas certas com conhecimento dos objectivos do teste

Estes resultados são bastante positivos, e mostram que quando a maioria das pessoas são motivadas para memorizar esta informação visual, conseguem posteriormente recuperá-la de forma eficaz.

Como os participantes foram informados dos objetivos do teste, então eles tentaram memorizar as posições e os tamanhos dos segmentos de reta desenhados, de uma forma muito mais consistente do que no caso do teste 1. Os resultados positivos apresentados deveram-se, provavelmente, ao facto de os participantes terem criado os seus próprios padrões no desenho dos traços sobre a imagem, o que lhes permitiu uma memorização mais eficaz. Isto permite concluir que este modelo de senha gráfica para a Web tem potencial para ser viável na utilização em mecanismos de autenticação.

No **teste 3,** os participantes tentaram reproduziram, sobre a mesma imagem, os seis segmentos de reta, que tinham registado 72 horas antes. Neste caso, pretendeu-se aferir o nível de memorização dos participantes num período de mais longa duração.

Como se pode analisar na Figura 9, 67,9% (dezanove em vinte e oito) dos participantes acertaram a posição dos seis segmentos de retas. Mas, por outro lado, quatro utilizadores (14,2%) não acertaram em qualquer um dos segmentos de reta. Isto pode indiciar que haverá um leque de pessoas, que poderá ter dificuldades na memorização deste tipo de informação gráfica. Isto pode motivar encontrar novas soluções, que podem passar por disponibilizar pistas visuais nas imagens de fundo da senha, que ajudem estes tipos de utilizadores a melhor memorizar os traços registados.

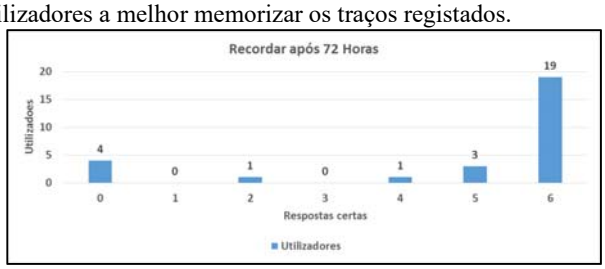

Figura 9 – Resultados do teste de memória de longa duração

Estes resultados permitem concluir que os elementos usados neste modelo de senha gráfica (seis segmentos de reta), podem oferecer aos seus utilizadores, uma reprodução eficaz dos traços registados previamente, indiciando que este modelo explora todo o potencial da memória visual. Os resultados mostram que não existe uma diferença significativa na eficácia da reprodução de todos os traços após o seu registo, para um período de 6h (64,3%), e de 72h (67,9%). Verificou-se também que houve uma evolução nos resultados dos utilizadores (entre o primeiro e terceiro teste). Isto indicia que quanto maior for a frequência de utilização do sistema, mais fácil de usar e mais eficaz ele se torna para os seus utilizadores. Os resultados anteriores mostram que este modelo de senha gráfica, tem potencial para ser usado em mecanismos de autenticação na Web.

5 Conclusões e Trabalho Futuro

A senha alfanumérica pode ser descoberta com alguma facilidade, por um espião de ombro, porque ele pode perceber facilmente que um utilizador está a realizar uma tarefa de autenticação, com base no padrão comum de interface gráfica que é usada para esse efeito. Esta evidência foi validada num teste exploratório, realizada no âmbito desta investigação, com quarenta e nove participantes, que simularam ser espiões de ombro. No caso em que um utilizador simulou o uso de uma senha gráfica sobre uma imagem, nenhum desses participantes suspeitou que ele estava a fazer uma tarefa de autenticação.

Estas conclusões levaram à convicção de que o uso de senhas gráficas pode despistar os espiões de ombro, quando o utilizador está a realizar as tarefas de autenticação. Esta questão motivou este trabalho a tentar encontrar um novo modelo de senha gráfica, no contexto dos sítios e aplicações Web, que assegurasse segurança e que fosse usável para o seu utilizador, constituindo-se uma proposta alternativa para substituir a senha alfanumérica.

Para desenhar esse modelo de senha gráfica sobre a Web, foram desenvolvidas várias versões iterativas, baseadas num conjunto de elementos orientadores: (i) uma imagem de fundo, gerada automaticamente a partir de uma página, do sítio Web em causa, (ii) e o desenho de um determinado número de objetos gráficos sobre a referida imagem.

Na primeira versão de desenho da senha gráfica, podiam ser desenhados oito objetos gráficos, de três tipos distintos: segmentos de reta, polígonos e círculos. O teste com participantes demonstrou que esse modelo provocou ao utilizador algumas dificuldades de memorização, relativas à geometria dos objetos, ao seu posicionamento e à sua sequência. Para reduzir esses problemas, decidiu-se que o utilizador só pode usar seis segmentos de reta, validados através das coordenadas dos seus pontos extremos.

Sobre esta última versão do modelo da senha, foram efetuados três testes com participantes. No primeiro teste, os participantes tentaram reproduzir a senha gráfica, passados seis horas após o seu registo. Pelo facto de não terem sido avisados para a sua reprodução, a esmagadora maioria teve muita dificuldade em lembrar-se da posição e do tamanho dos traços registados.

No segundo teste, um outro grupo de participantes já foi informado durante o registo da senha gráfica, de que deveria memorizá-la e reproduzi-la 6h depois. A eficácia na reprodução dos seis traços, foi muito superior ao teste

anterior, o que mostrou que a memorização aumenta quando o utilizador é motivado para a tarefa.

O terceiro teste, semelhante ao anterior, solicitou a reprodução da senha gráfica, 72h após o seu registo. Os resultados permitiram concluir que este modelo de senha gráfica ofereceu no geral, uma reprodução eficaz dos traços registados. É importante referir que os resultados mostram que não existe uma diferença significativa na eficácia na reprodução dos traços, em períodos de tempo de média duração (6h), e de mais longa duração (72h), após o seu registo. Verificou-se também que houve uma evolução nos resultados dos utilizadores (entre o primeiro e terceiro teste). Isto indicia que quanto mais os participantes utilizarem o sistema, maior é o seu desempenho. Todos estes argumentos anteriores mostram que este modelo de senha gráfica tem potencial para ser usado em mecanismos de autenticação Web.

Através de um inquérito aplicado aos participantes, percebeu-se quais foram as principais pistas visuais que eles usaram sobre a imagem de fundo. Esta funciona como mnemónica que permite reconhecer melhor a posição e o tamanho dos traços registados previamente.

Já está em implementação um mecanismo de autenticação que usa este modelo de senha gráfica. Pretende-se confrontá-lo com o método tradicional que é suportado numa senha alfanumérica.

Na sequência desse trabalho, está-se a tentar descobrir qual é a tolerância do erro (em pixel), entre os traços que os utilizadores registam e a sua reprodução no processo de autenticação, por forma a assegurar a maior eficácia possível, sem comprometimento da segurança do sistema. Para tal, estão a ser tidos em conta a inclinação e as coordenadas das posições extremas dos segmentos de reta. Estão igualmente a ser desenhados testes com utilizadores para se descobrir a diferença de desempenho do utilizador, entre o modelo de senha alfanumérica tradicional e o deste modelo proposto de senha gráfica.

6 Referências

[1] Dinei Florencio and Cormac Herley. 2007. A large-scale study of web password habits. In Proceedings of the 16th international conference on World Wide Web (WWW '07). ACM, New York, NY, USA, 657-666.

[2] 12 best Android lock screen apps and widgets to reinvent your phone , “https://www.androidpit.com/best-android-lock-screen-apps”, acedido pela ultima vez em Janeiro de 2015.

[3] Microsoft Personalize you PC http://windows.microsoft.com/en-US/windows-8/picture passwords?woldogcb=0, acedido pela ultima vez em Janeiro de 2015.

[4] Robert Biddle, Sonia Chiasson, and P.C. Van Oorschot. 2012. Graphical passwords: Learning from the first twelve years. ACM Comput. Surv. 44, 4, Article 19 (September 2012), 41 pages.

[5] Segurança de senhas alfanuméricas “http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-pt_br-4/s1-wstation-pass.html” , acedido pela ultima vez em Janeiro de 2015.

[6] Senhas Alfanuméricas Fortes “http://windows.microsoft.com/pt-BR/windows-vista/Tips-for-creating-a-strong-password” , acedido pela ultima vez em Janeiro de 2014.

[7] Secure, Visual Data Security White Paper - Brian Honan, BH Consulting July 2012.

[8] D. Hong, S. Man, B. Hawes, and M. Mathews, "A Password scheme strongly resistant to spyware," in Proceedings of International conference on security and management. Las Vergas, NV, 2004.

[9] S. Man, D. Hong, and M. Mathews, "A shouldersurfing resistant graphical password scheme," in Proceedings of International conference on security and management. Las Vegas, NV, 2003.

[10] I. Jermyn, A. Mayer, F. Monrose, M. K. Reiter, and A. D. Rubin, "The Design and Analysis of Graphical Password," in Proceedings of the 8th USENIX Security Symposium, 1999.

[11] J. Goldberg, J. Hagman, and V. Sazawal, "Doodling Our Way to Better Authentication," presented at Proceedings of Human Factors in Computing Systems (CHI), Minneapolis, Minnesota, USA., 2002.

[12] A. F. Syukri, E. Okamoto, and M. Mambo, "A User Identification System Using Signature Written with Mouse," in Third Australasian Conference on Information Security and Privacy (ACISP): Springer-Verlag Lecture Notes in Computer Science (1438), 1998, pp. 403-441.

[13] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical password” , 2005

[14] Xiaoyuan Suo; Ying Zhu; Owen, G.S., "Graphical passwords: a survey," Computer Security Applications Conference, 21st Annual , vol., no., pp.10 pp.,472, 5-9 Dec. 2005 doi: 10.1109/CSAC.2005.27

[15] J.-C. Birget, D. Hong, and N. Memon, "Robust discretization, with an application to graphical Password," Cryptology ePrint archive 2003.

[16] A. Perrig and D. Song, "Hash Visualization: A New Technique to Improve Real-World Security," in Proceedings of the 1999 International Workshop on Cryptographic Techniques and E-Commerce, 1999.

[17] Rachna Dhamija and Adrian Perrig. 2000. Déjà Vu: a user study using images for authentication. In Proceedings of the 9th conference on USENIX Security Symposium - Volume 9(SSYM'00), Vol. 9. USENIX Association, Berkeley, CA, USA, 4-4.

[18] D. Weinshall and S. Kirkpatrick, "Senhas You’ll Never Forget, but Can’t Recall," in Proceedings of Conference on Human Factors in Computing Systems (CHI). Vienna, Austria: ACM, 2004, pp. 1399-1402.

[19] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13th Usenix Security Symposium. San Diego, CA, 2004.

[20] L. Sobrado and J.-C. Birget, "Graphical passwords," The Rutgers Scholar, An Electronic Bulletin for Undergraduate Research, vol. 4, 2002.

[21] J. Thorpe and P. C. v. Oorschot, "Graphical Dictionaries and the Memorable Space of Graphical Password," in Proceedings of the 13th USENIX Security Symposium. San Deigo, USA: USENIX, 2004.

[22] X.Y. Liu., J.H. Qiu., L.C. Ma., H.C. Gao., etc., “A Novel Cued-recall Graphical Password Scheme”, In sixth International Conference on Image and Graphics (ICIG), 2011.

[23] Eluard, M.; Maetz, Y.; Alessio, D.; , “Action-based graphical password: Click-a-Secret”, 2011 IEEE International Conference on Consumer Electronics, 2011, pp.

[24] D. Nali and J. Thorpe, "Analyzing User Choice in Graphical Password," Technical Report, School of Information Technology and Engineering, University of Ottawa, Canada May 27 2004.

[25] G. E. Blonder, "Graphical Password," in Lucent Technologies, Inc., Murray Hill, NJ, U. S. Patent, Ed. United States, 1996.

[26] Passlogix, "www.passlogix.com" acedido pela ultima vez em Setembro de 2013.

[27] “Signing in with a picture password” , in Building Windows 8 in the MSDN Blogs, http://blogs.msdn.com/b/b8/archive/2011/12/16/signing-in-with-a-picture-password.aspx , acedido pela ultima vez em Junho de 2015.

[28] L. D. Paulson, "Taking a Graphical Approach to the Password," Computer, vol. 35, pp. 19, 2002.

[29] 22nd USENIX Security Symposium.August 14–16, 2013 • Washington, D.C., USA ISBN 978-1-931971-03-4 graphical password," Cryptology ePrint archive 2003.

[30] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "PassPoints: Design and longitudinal evaluation of a graphical Password system," International Journal of Human Computer Studies, to appear.

[31] P. C. van Oorschot, A. Salehi-Abari and J. Thorpe. “Purely Automated Attacks on PassPoints-Style Graphical Passwords”. IEEE Transactions on Information Forensics and Security, 2010.

[32] R Padmavathy, Chakravarthy Bhagvati. “A Small Subgroup Attack for Recovering Ephemeral Keys in Chang and Chang Password Key Exchange Protocol”. Journal of Computers, vol.6, no.4, 2011.

[33] Zuowen Tan. “An Authentication and Key Agreement Scheme with Key Confirmation and Privacy-preservation for Multi-server Environments”, Journal of Computers, vol.6, no.11, 2011.

[34] Engenharia Social “http://pt.wikipedia.org/wiki/Engenharia_social” acedido pela ultima vez em Janeiro de 2015.

[35] S. Wiedenbeck, J. Waters, J. C. Birget, A. Brodskiy, and N. Memon, "Authentication using graphical Password: Basic results," in Human-Computer Interaction International (HCII 2005). Las Vegas, NV, 2005.